REMARKS

I. The Cited reference and the Subject Invention

A. The Fischer Reference

U.S. Patent No. 5,659,617 to Fischer (hereinafter "the Fischer reference") discloses a method and apparatus for providing location certificates to certify the position or location of an object. The position of the object is computed using radio signals, and secure transmission of the computed position is achieved using public key encryption techniques. In particular, the Fischer reference uses a pre-designed encryption key to *encrypt location information*. The Fischer reference stores a private key in the secure authorization unit (SAU) memory for use in encrypting messages. The corresponding public key is disseminated to other requestors for use in decrypting messages encrypted using the stored private key. (See Fischer FIG. 1, col. 3, lines 4-15). In response to a request, the location certification unit (LCU) computes its current location and sends the location and a certificate to the requestor encrypted using its private key. (See Fischer, col. 3. lines 40-50). The requestor then verifies the message by decrypting the message using the corresponding public key and checking the received location information. (See Fischer, col. 3. lines 50-61).

B. The Subject Invention

Embodiments of the present invention protect electronic files utilizing an environment profile that describes the operating environment of the client computer, which can include such factors as the geo-location of the computer, drive ID(s), electronic address assignments, and time and date ranges. Since this environment information is utilized to protect electronic files, only a client computer conforming to the operating environment as defined in the profile can access data files protected using the embodiments of the present invention. (See application as filed page 33, lines 8-13). When protecting an electronic file, the operating environment of the computer is obtained and utilized to *generate an encryption key*, which then is used to encrypt an electronic file. To decrypt the file at a later date, the same encryption key needs to be regenerated. However, if any factor of the environment profile changes, the regenerated key will be different from the key used to encrypt the file because the environment profile on which the regenerated key is based will be different. As a result, the regenerated key will be unable to decrypt the file.

II. Claim Rejections - 35 USC §102

The Examiner rejected claims 1-6, 15-22, and 26-33 under 35 U.S.C. §102(e) as being anticipated by the Fischer reference. The Applicant respectfully traverses this rejection. Nowhere in any of the cited references is there disclosed or reasonably suggested the operation of *generating an encryption key based on the environment information*, as required by independent claim 1. Independent claim 1 requires obtaining environment information that includes data regarding the operating environment of a computer, and utilizing the environment information to *generate* an encryption key, which is used to encrypt an electronic file.

The *encryption key is actually generated based on the environment information* of the computer. As illustrated in Fig. 12 of the application as filed, embodiments of the present invention append the environment information, in the form of an environment profile, to a user passphrase and then create a public and private key pair from the combined passphrase and environment information. (See application as filed page 35, lines 5-17, FIG. 12). Thus, if there are any changes to the environment information of the computer, the generated encryption key will change.

Once the encryption key is generated, the file is encrypted. To access the file at a later date, a new encryption key needs to be generated as before. However, if there are any changes to the environment information of the computer, the generated encryption key will change, and thus be unable to decrypt the file. For example, if the encrypted file is moved to another computer, the environment information of the other computer will not match the environment information used to generate the encryption key which was used to encrypt the file. As a result, when the other computer generates the new encryption key, the generated encryption key will not be able to decrypt the file, hence protecting the file from unauthorized access.

The Fisher reference does not disclose using computer environment information to *generate an encryption key*. In contrast, the Fisher reference uses a pre-designed encryption key to *encrypt location information*, but does not disclose *generating an encryption key based on the environment information*, as required by independent claim 1.

Accordingly, independent claim 1 is submitted to be patentable under 35 U.S.C. § 102 over the Fischer reference. Claims 2-14, each of which ultimately depends from independent claim 1, are

likewise submitted to be patentable under 35 U.S.C. § 102 over the Fischer reference for at least the same reasons set forth above regarding claim 1.

Independent claim 15 requires storing an electronic file encrypted using an encryption key. Similar to claim 1 above, the encryption key is generated using a first environment profile, which includes data regarding the operating environment of a computer. Hence, independent claim 15 requires the encryption key to be *generated based on the environment profile.* Independent claim 15 further requires obtaining a second environment profile of the computer based on the current operating environment of the computer. A decryption key is generated based on the second environment profile and used to decrypt the electronic file.

As stated above, the second environment profile is utilized to generate the decryption key. However, if there are any changes to the operating environment of the computer, the second environment profile will be different from the first environment profile. As a result, the generated decryption key will change and be unable to decrypt the electronic file. As stated above, the Fisher reference does not disclose using a computer environment profile to *generate an encryption key and a decryption key.* Thus, for these reasons and the reasons set forth above with reference to independent claim 1, the Fischer reference cannot anticipate independent claim 15.

Accordingly, independent claim 15 is submitted to be patentable under 35 U.S.C. § 102 over the Fischer reference. Claims 16-25, each of which ultimately depends from independent claim 15, are likewise submitted to be patentable under 35 U.S.C. § 102 over the Fischer reference for at least the same reasons set forth above regarding claim 15.

Independent claim 26 also requires, *inter alia*, generating an encryption key based on the environment information and encrypting an electronic file using the encryption key. As set forth above with reference to claims 1 and 15, the Fisher reference does not disclose using a computer environment information to *generate an encryption key.* Accordingly, independent claim 26 is submitted to be patentable under 35 U.S.C. § 102 over the Fischer reference for at least the reasons set forth above with reference to claims 1 and 15. Claims 27-38, each of which ultimately depends from independent claim 26, are likewise submitted to be patentable under 35 U.S.C. § 102 over the Fischer reference for at least the same reasons set forth above regarding claims 1, 15, and 26.

In view of these remarks and the above amendments, allowance of this application is believed to be in order, which action is respectfully requested. If any discussion of this application is initiated by the Examiner, please direct a call to **Joe A. Brock II, Esq., 909-624-8880 x102.**

Respectfully submitted,

PATENT VENTURE GROUP
333 N. Indian Hill Blvd., Suite 208
Claremont, CA 91711
(909) 624-8880 x102
Fax: (888) 847-2501

By: _____
Name: Joe A. Brock II, Esq.
Reg. No.: 46,021
Date: Oct. 26, 2004